

# User Guide

---

NC-PASS Authenticator  
Version 2.0

MVS Operating Environment

© Copyright 2001 PassGo Technologies Ltd. All rights reserved.  
Proprietary and Confidential Information of PassGo Technologies Ltd.

Publication number PAU0001.003

Third Edition (October 2001)

Published by:

PassGo Technologies Ltd, Horton Manor, Ilminster, Somerset, TA19 9PY, England.

This book refers to a number of hardware and software products that are produced by other companies. In most, if not all cases, the names of these products are claimed as trademarks by the companies that manufacture them. It is not our intention to claim either the products or their names or trademarks as our own.

Changes will be made periodically to the information contained in this book. If your book does not accurately reflect the level of product you are using, this may be due to a fix being applied to the product which has still to be released as a book update.

## Preface

### **Purpose of this book**

This book shows you how to use the various authentication devices supported by NC-PASS. It explains data entry procedures and provides step by step descriptions for gaining access to your system using the various devices.

### **Who should read this book**

This book is intended for users who want to use NC-PASS Authenticator with an associated authentication token to gain access to their computer system.

### **Readers' comment forms**

Forms for readers' comments are provided at the back of this manual.

Any information you return may be used or distributed by the authors in any manner considered appropriate without incurring any obligation whatsoever.

*This page intentionally left blank*

## **Table of contents**

Preface

Chapter 1 Using tokens

Chapter 2 The SecurID A token

Chapter 3 The SecurID P token

Chapter 4 The ActivCard token

Chapter 5 The Digipass token

Chapter 6 The Watchword token

Chapter 7 The CRYPTOCARD token

Chapter 8 The SecureNet Key token

Chapter 9 The Safe S220 token

Chapter 10 Token registration and replacement

Index

*This page intentionally left blank*

# Chapter 1 - Using tokens

- Introduction .....1.2
  - Tokens .....1.2
  - Using passcodes .....1.3
  - Logging on from a different location to normal .....1.3

---

## Introduction

Your computer system is protected by a security product called NC-PASS. This product allows authorized users to gain access to the computer, but stops and reports attempts to gain access illegally.

This user guide is intended to show you, the authorized user, how to gain access to your computer system.

## Tokens

Your administrator may have provided you with a token; if so, you will need this token to gain access to your computer system under circumstances defined by your administrator. For example, you may have to use it:

- every time you logon to your computer
- to authorize you to perform a particular function
- to gain access from a particular terminal
- at specific dates or times.

This token is your personal security device; you should ensure that you keep it safe at all times.

Each token is described in a separate chapter, and specific operating instructions are provided in every case.

It is assumed that each token has been initialized (if necessary) by the administrator.

As initialization procedures vary from token to token, the initial input requirements also vary. One of the first requirements could be to install a PIN in the token. PIN installation can, however, be part of the initialization process and an administrator may then issue a token with an initial PIN already installed. In this case you may have to install a new PIN so that only you know the number. The instructions provided in this User Guide therefore reflect the individual requirements of each token type.

### Using a token at logon

When logging on, you are normally asked to enter your userid and password.

If you have a token, you may then be asked to provide details from the token; if your userid, password and token details are correct, you will be allowed to access your system.

### Using a token at other times

You may be asked for token details at times other than when you are logging on; for example, you may be asked for token details when you try to process a particular transaction.

### Assigning yourself to a token

Every token has a unique number. A record is kept on the computer detailing which userids are assigned to which tokens. When your administrator gives you your token, he will tell you whether you will have to register your token, or whether he has done this for you.

If you have to register your token yourself, refer to *Registering your token* on page 10.2.

## Token expiry

After you have been using your token for some time, your administrator may provide you with a new token. You will be prompted by the system to provide details of the new token. Refer to *Replacing your old token with a new token* on page 10.3.

## Using passcodes

An optional feature of NC-PASS authentication is the passcode facility which can be used to provide an additional level of security at logon when using tokens. Instead of simply entering a userid and token response code at the logon panel, you are asked to enter a passcode consisting of a PIN, a delimiter and a response code as follows:

PIN / token response

The extra security is provided by the passcode PIN which is generated by NC-PASS at initial logon (not to be confused with the token PIN).

To generate a PIN at initial logon, you must enter the token type and serial number in place of the PIN number (followed by the delimiter and response code) as follows:

type / token serial number / code

NC-PASS will allocate a unique PIN to the token serial number and display this on the screen. The PIN must then be noted for subsequent entry as part of the passcode.

As the passcode feature is optional, the logon procedures described in subsequent chapters of this User Guide reflect normal response processing (ie without passcode).

## Logging on from a different location to normal

A company may have many linked computers, eg one at headquarters in New York and one at the London office. If a user normally works from the New York office, but occasionally needs to travel to the London office, he may still require access to his usual computer applications.

If this situation applies to you, NC-PASS can allow you to use a terminal at a site other than your normal location, eg London, specifying the name of your 'home' computer, eg NewYork, when you logon. (Your administrator will advise you if this facility has been set up and if so, the 'name' of your home computer.)

Enter your userid, password and token details, as normal. If the information you supply is correct, you should gain access to your usual applications.

*This page intentionally left blank*

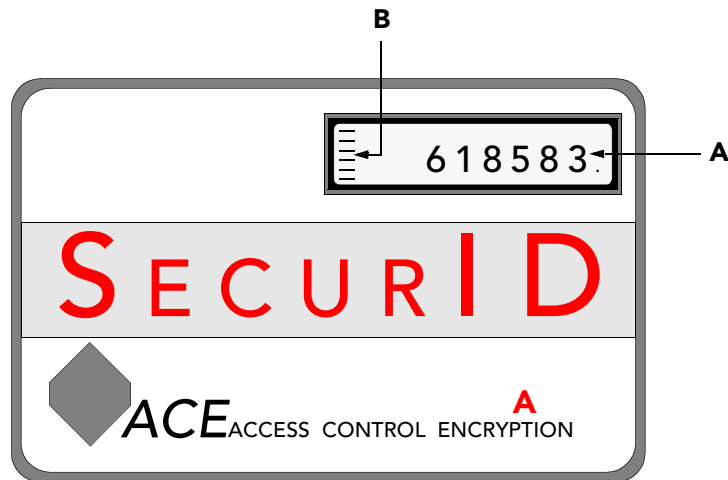
## Chapter 2 - The SecurID A token

|   |     |
|---|-----|
| SecurID A token description .....         | 2.2 |
| Using the token .....                     | 2.3 |
| Logging on with the SecurID A token ..... | 2.3 |

---

## SecurID A token description

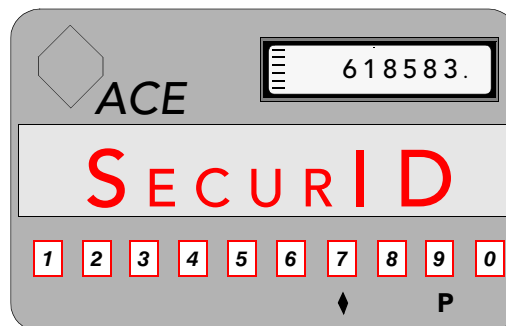
Your administrator has provided you with a token called the SecurID A token, similar to the token shown below. You will need this token to gain access your computer system, as defined by your system administrator.



The components of the token are described below.

- A a random number display, known as the PRN (Pseudo Random Number). This number changes after a set period of time.
- B indicator bars showing how much time is left in this period. 6 bars are displayed at the start of the period, no bars at the end.

**Note:** If your token has a numeric keypad, similar to the one shown below, refer to *Chapter 3 - The SecurID P token*.



## Using the token

Your administrator will tell you when you must use the token. You may have to use it:

- every time you logon to your computer
- to authorize you to perform a particular function
- to gain access from a particular terminal
- at specific dates or times.

The following section describes how you would use the token to logon to your computer - if you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure.

## Logging on with the SecurID A token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

To access your computer system from your logon panel, carry out the steps on the following page.

---

**Step 1** Enter your USERID and, if required, a PASSWORD. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

**Step 2** If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

**Step 3** Read the display (A) from your SecurID token.

**Step 4** Enter the displayed number at the PRN prompt on your terminal and press <Enter>.

You should now gain access to your computer system. If you receive an information message, an example of which is shown below, follow the instructions in the message.

```
*****
|
| Your token expires in 5 days. Please contact your administrator if you do
| not receive your replacement token.
|
|
```

---

CKSE2425-9 Press Enter to Continue or F6 to register new token

If you are asked to register a new token, refer to *Replacing your old token with a new token* on page 10.3.

---

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

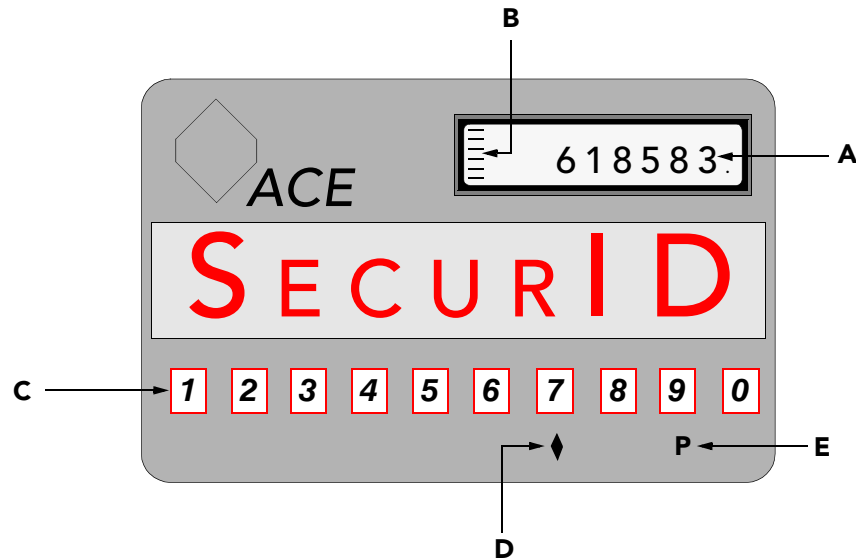
## Chapter 3 - The SecurID P token

|   |     |
|---|-----|
| SecurID P token description .....         | 3.2 |
| Using the token .....                     | 3.3 |
| Setting up the initial PIN .....          | 3.4 |
| Changing the PIN .....                    | 3.5 |
| Logging on with the SecurID P token ..... | 3.5 |
| Token expiry .....                        | 3.6 |

---

## SecurID P token description

Your administrator has provided you with a token called the SecurID P token similar to the token shown below. You will need this token to gain access your computer system, as defined by your system administrator.



The components of the token are described below.

- A a random number display, known as the PRN (Pseudo Random Number). This number changes after a set period of time.
- B indicator bars showing how much time is left in this period. 6 bars are displayed at the start of the period, no bars at the end.
- C the numeric keypad. This can be used to enter a Personal Identification Number (PIN) if one is required. A PIN is a secret number known only to you.
- D the <Enter> or <Return> key.
- E the clear key.

This token can be used with or without a Personal Identification Number (PIN). A PIN is a secret number known only to you. Your administrator will tell you if you must use a PIN and if so, how many letters/numbers your PIN can contain.

**Note:** The letters used in this diagram, pointing to the various parts of the token, are used in the following text to identify the relevant area.

---

## Using the token

Your administrator will tell you when you must use the token.

The following sections describe how you would use the token to logon to your computer - if you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure.

The following questions and answers will guide you to the appropriate sections. If in doubt, contact your administrator.

**Q1** Do you have a PIN to use with the token?

**A1** Yes - go to Q2.

Yes, but I have forgotten it - contact your administrator.

No - go to Q3.

**Q2** Do you want to change it now?

**A2** Yes - go to the section entitled *Changing the PIN* on page 3.5.

No - go to the section entitled *Logging on with the SecurID P token* on page 3.5

**Q3** Do you want to add a PIN? (Your administrator may specify that you **must** use a PIN.)

**A3** Yes - go to the section entitled *Setting up the initial PIN* on page 3.4

No - go to the section entitled *Logging on with the SecurID P token* on page 3.5.

## Setting up the initial PIN

Follow the steps listed below to install the initial PIN for your SecurID P token:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Carry out the necessary procedure to display the logon panel for your computer system on your terminal. For details refer to <i>Logging on with the SecurID P token</i> on page 3.5.   |
| <b>Step 2</b> | Enter your USERID and, if required, a PASSWORD. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)   |
| <b>Step 3</b> | <p>You may be presented with a panel asking you to register your use of the token. If so, go to <i>Registering your token</i> on page 10.2, carry out the steps there, before returning to complete step 4.</p> <p>If you have not been asked for registration details, carry on with Step 4.</p>  |
| <b>Step 4</b> | <p>Your terminal will display</p> <ul style="list-style-type: none"><li>• a prompt asking for the PRN or token display number - Enter the random number from the token (A)</li><li>• a prompt asking you to enter a new PIN - enter a PIN of your choice</li><li>• a prompt asking you to verify the new PIN - enter the same PIN again to verify you have entered it correctly. Remember this number as you will need it for subsequent logons.</li></ul> |
| <b>Step 5</b> | Press the <Enter> key on your terminal. You should now have gained access to your computer system. If you receive an information message, follow the instructions in the message. For subsequent logons, follow the steps described in <i>Logging on with the SecurID P token</i> on page 3.5.   |
- 

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

## Changing the PIN

Follow the steps listed below to change the PIN for your SecurID P token. You must know the current PIN.

- Step 1** Carry out the necessary procedure to display the logon panel for your computer system on your terminal. For details refer to *Logging on with the SecurID P token* on page 3.5.
- Step 2** Enter your USERID and, if required, a PASSWORD.
- Step 3** On your token, use the keypad (C) to enter your current PIN. Press the diamond shape (D) to enter the PIN on the token. A new random number will be displayed on your token (A). Type this number at the PRN prompt on your terminal.
- Step 4** Enter a PIN of your choice at the New PIN prompt on your terminal.
- Step 5** Enter the same PIN again to verify you have entered it correctly. Remember this number as you will need it for subsequent logons.
- Step 6** Press the <Enter> key on your terminal. You should now have gained access to your computer system. If you receive an information message, follow the instructions in the message. For subsequent logons, follow the steps described in *Logging on with the SecurID P token* on page 3.5.

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

## Logging on with the SecurID P token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

---

**Step 1** Enter your USERID and, if required, a PASSWORD. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

**Step 2** If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

**Step 3** On your token, use the keypad (C) to enter your current PIN. Press the diamond shape (D) to enter the PIN on the token. A new random number will be displayed on your token (A). Type this number at the PRN prompt on your terminal.

Press the <Enter> key on your terminal. You should now have gained access to your computer system. If you receive an information message, an example of which is shown below, follow the instructions in the message.

```
*****
|
| Your token expires in 5 days. Please contact your administrator if you do |
| not receive your replacement token. |
|
|
```

---

CKSE2425-9 Press Enter to Continue or F6 to register new token

If you are asked to register a new token, refer to *Replacing your old token with a new token* on page 10.3.

---

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

## Token expiry

Each SecurID P token has a 'death date' on which it will expire, programmed into it during manufacture. Your administrator should set up a warning message which will appear before the death date. The administrator sets how many days in advance of the death date the warning appears. When you receive this message, contact your administrator who should issue you with a new token. See the section entitled *Registering your token* on page 10.2 for further details.

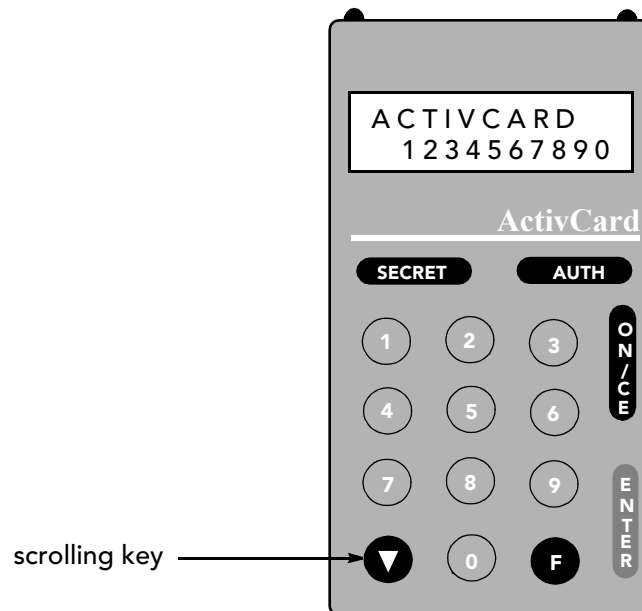
## Chapter 4 - The ActivCard token

|   |     |
|---|-----|
| ActivCard token description .....         | 4.2 |
| Using the token .....                     | 4.3 |
| Setting up the initial PIN .....          | 4.3 |
| Changing the PIN .....                    | 4.3 |
| Logging on with the ActivCard token ..... | 4.4 |
| Card locked .....                         | 4.6 |


---

## ActivCard token description

Your administrator has provided you with a token called the ActivCard token similar to the token shown below. You will need this token to gain access to your computer system, as defined by your system administrator.



The keys required to use the token are described below.

- |   |   |
|---|---|
| <b>AUTH</b>   | displays the ActivCard Authentication menu.   |
| <b>ON/CE</b>  | switches the ActivCard token on, clears the last entry and returns to the previous screen or procedure. |
| <b>ENTER</b>  | stores the contents of the display and displays the next screen.  |
| <b>F</b>  | displays the ActivCard service menu.  |
|  | scrolls between screens on a menu.  |
| <b>SECRET</b>   | not supported by NC-PASS.   |

This token must be used with a Personal Identification Number (PIN). The maximum and minimum lengths of the PIN are defined by the administrator during initialization. The PIN is a secret number known only to you.

If you suspect that someone else knows your PIN you must change it, as described in the *ActivCard X9.9 Token User Guide*, supplied with your token.

If you make no entries to your ActivCard for 30 seconds, it will automatically switch itself off.

---

## Using the token

Your administrator will tell you when you must use the token.

The following sections describe how you would use the token to log on to your computer. If you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure.

The following questions and answers will guide you to the appropriate sections. If in doubt, contact your administrator.

**Q1** Is this the first time you have used the token?

**A1** Yes - refer to the *ActivCard X9.9 Token User Guide*, supplied by ActivCard Networks Inc.

No - go to Q2 below.

**Q2** Do you want to change your PIN?

**A2** Yes - refer to the *ActivCard X9.9 Token User Guide*, supplied by ActivCard Networks Inc.

No - go to *Logging on with the ActivCard token* on page 4.4.

### Setting up the initial PIN

Before you can use your token, you must enter an initial Personal Identification Number (PIN) into the token. A PIN is a number known only to you and should not be disclosed to anyone else.

While you are setting up your initial PIN, you may be presented with a message asking you to register your use of the token. If so, go to *Registering your token* on page 10.2 and carry out the steps there before continuing to set the initial PIN.

How to install the initial PIN for your ActivCard token is described in the *ActivCard X9.9 Token User Guide*, supplied with your token.

### Changing the PIN

To change the PIN for your ActivCard token, for example because you think someone else knows it, follow the instructions in the *ActivCard X9.9 Token User Guide* supplied with your token. You must know the current PIN.

## Logging on with the ActivCard token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

To access your computer system from your logon panel, carry out the following steps:

- Step 1** Enter your **USERID** and, if required, a **PASSWORD**. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

**Step 2** If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

**Step 3** If your logon panel has a **Challenge** field, a **Challenge** number is then issued.

**Step 4** Press the **ON/CE** key on the token. The display shows a message and the token's internal serial number. (If the message is **NEW CARD**, you need to set up the initial PIN as described in your *ActivCard X9.9 Token User Guide*.) After a few seconds, the token display will prompt you to enter the PIN.

ENTER PIN

-----

## Step 5

Enter your current PIN on your token and press **ENTER**. For security reasons, dashes (-) are displayed in place of the actual decimal digits entered.

## Step 6

Select the token slot advised by your administrator by pressing the scrolling key until the correct slot, eg PASS, is displayed and then press **ENTER**.

## Step 7

You are then prompted to select A, S or F. Select A by pressing the AUTH key.

## Step 8

If you have been set up for challenge/response mode, the token displays the CHALLENGE prompt. Enter the Challenge displayed on your logon panel into your token and press **ENTER** to display the dynamic password in decimal or hexadecimal characters.

If you have been set up for response only mode, the token displays the dynamic password when you press the AUTH key.

## Step 9

Press the **ENTER** key on your token to swap between decimal and hexadecimal displays. A lower case **d** or **h** character indicates which form of dynamic password is being displayed (in this case, decimal).

Example only

If the dynamic password exceeds 12 characters in length, the triangular symbol appears. If this occurs, press the scrolling key to display the rest of the dynamic password. The **d** or **h** indicator will be followed by a number indicating which part of the display is being shown on the token, eg 1 for the first part as shown.

Example only

## Step 10

Enter the dynamic password from your token at the **Response** prompt (do **not** include spaces). You can enter either the hexadecimal or decimal number. Press Enter. You should now have gained access to your computer system.

If you are asked if you want to register a new token, refer to *Replacing your old token with a new token* on page 10.3.

If you receive a message telling you that your password has expired, respond to the prompts following the message.

---

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to log on again. If you do not know why you have been denied access, contact your administrator for advice.

---

## Card locked

If you enter an incorrect PIN, your token will display PIN ERROR *n* where *n* indicates how many incorrect PINs you have entered since the last correct one.

The administrator has set up the number of incorrect PINs you can enter before your card becomes locked and unusable.

When you have a single attempt remaining before your token will lock, the following message will be displayed - LAST PIN TRY and you must press ENTER to continue. If you enter another incorrect PIN the token will become locked and display CARD LOCKED.

**WARNING:** If your token does become locked (the display reads CARD LOCKED), contact your system administrator who will unlock it for you. Do not attempt to use it or all the parameters set up for it during initialization will be erased.

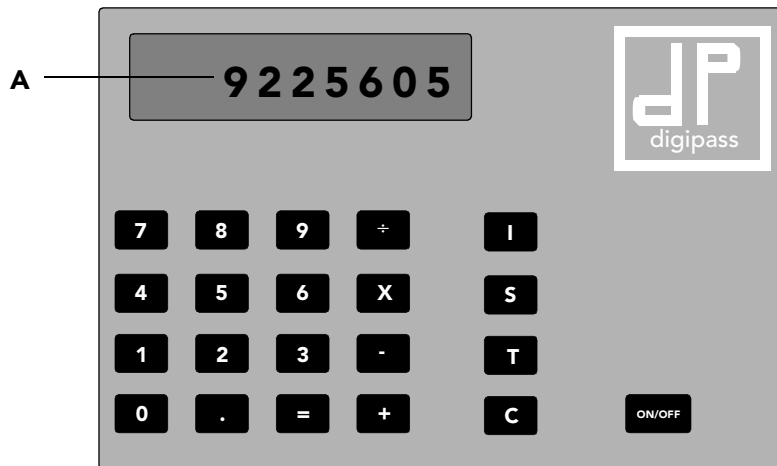
## Chapter 5 - The Digipass token

|  |     |
|--|-----|
| Digipass token description .....         | 5.2 |
| Using the token .....                    | 5.3 |
| Changing the initial PIN (IPIN) .....    | 5.4 |
| Logging on with the Digipass token ..... | 5.5 |

---

## Digipass token description

Your administrator has provided you with a token called the Digipass token similar to the token shown below. You will need this token to gain access to your computer system, as defined by your system administrator.



The keys required to use the token are described below.

- I** generates an identification key.
- S** not supported in this release of NC-PASS.
- T** causes the Digipass to perform a self-test routine which checks that both the hardware and software is working correctly. For use by the administrator only.
- C** switches the Digipass token into Calculator mode, if the token was set up with calculator mode enabled.
- =** stores the contents of the display and displays the next screen.
- ON/OFF** switches the Digipass token on and off.

This token must be used with a Personal Identification Number (PIN). The Initial PIN (IPIN) is set up during the token's initialization.

Your administrator will tell you what the IPIN is and whether you can change it to a PIN of your choice. If you can change the PIN, do so by following the instructions in *Changing the initial PIN (IPIN)* on page 5.4. The new PIN should be a secret number known only to you. Your administrator will tell you how many numbers your PIN can contain.

---

## Using the token

Your administrator will tell you when you must use the token.

The following questions and answers will guide you to the appropriate sections, which describe how you would use the token to log on to your computer. If you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure. If in doubt, contact your administrator.

**Q1** Is this the first time you have used the card?

**A1** Yes - go to *Changing the initial PIN (IPIN)* on page 5.4.  
No - go to Q2.

**Q2** Do you remember your PIN?

**A2** Yes - go to Q3.  
No - contact your administrator.

# Changing the initial PIN (IPIN)

Before you can use your token, the administrator must have set up the token. You should then enter the IPIN, as provided by your administrator. Depending on the way your token was set up at initialization you may be able to change this to a PIN of your choice. This should be a number known only to you. Do not disclose it to anyone else.

Complete the steps below to change the initial PIN on your token.

|        |  |                             |
|--------|--|-----------------------------|
| Step 1 | Press the <b>ON/OFF</b> key on your token. The following screen will be displayed:   | <div>0</div>                |
| Step 2 | Press the <b>I</b> key. If your token has been set up to use only one application, the INIT PIN? prompt will be displayed (go to Step 3). If your token has been set up to use more than one application, scroll to the application advised by your administrator using the plus (+) and minus (-) keys. To select the required application, press the equals (=) key. | <div>application name</div> |
| Step 3 | The following message is displayed:  | <div>INIT PIN ?</div>       |
| Step 4 | Enter the IPIN supplied by the administrator for the given application. The following screen will be displayed.  | <div>PIN ?</div>            |
| Step 5 | Enter a new PIN of your choice and press the equals (=) key. Your administrator will advise you how long this should be. You will be prompted to repeat your PIN for verification purposes.  | <div>PIN ?</div>            |
| Step 6 | Enter the new PIN again and press the equals (=) key. The Digipass token will return to calculator mode.   | <div>0</div>                |

**WARNING:** Once you have set your PIN, do not forget it or let it become known to anyone else as you may not be able to change it, depending on the way your token was initialized. If you forget your PIN, contact your administrator.

## Logging on with the Digipass token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

To access your computer system from your logon panel, carry out the following steps:

## Step 1

Enter your **USERID** and, if required, a **PASSWORD**. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

## Step 2

If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

### Step 3

Press the **ON/OFF** key on your token. Press the **I** key. If your token has been set up to use only one application, the PIN? prompt will be displayed (go to Step 4).

If your token has been set up to use more than one application, scroll to the application advised by your administrator using the plus (+) and minus (-) keys. To select the required application, press the equals (=) key.

*application name*

### Step 4

The following message is displayed:

PIN ?

- Step 5** Enter the PIN for the selected application. The PIN is not shown on the token display panel, but is represented by asterisks (\*). (If you realize that you have made a mistake in entering your PIN press the **C** key and repeat this step.)
- \*\*\*\*\*
- Step 6** Press the equals (=) key. Three dots are displayed on the token while it is processing, then a six digit key.
- 3 1 2 6 4 5
- Example only**
- Step 7** Enter the identification key displayed on your token into the **Response** field on your logon panel and press Enter.
- An information message displaying a four digit number may be displayed. If it is, press the equals (=) key on your token to display a four digit number which must match the number displayed on your logon panel.
- If the numbers match, you should now have gained access to your computer system.
- If the numbers do not match, continue with Step 8 then log off and log on again. If it happens more than once, contact your administrator.
- Step 8** If you are asked if you want to register a new token, refer to *Replacing your old token with a new token* on page 10.3.
- If you receive a message telling you that your password has expired, respond to the prompts following the message.
- Step 9** Return the token to calculator mode, if applicable, by pressing the **C** key, or press the **ON/OFF** key.
- 

If you receive an error message, you may have entered incorrect data. Try to log on again. If you do not know why you have been denied access, contact your administrator for advice.

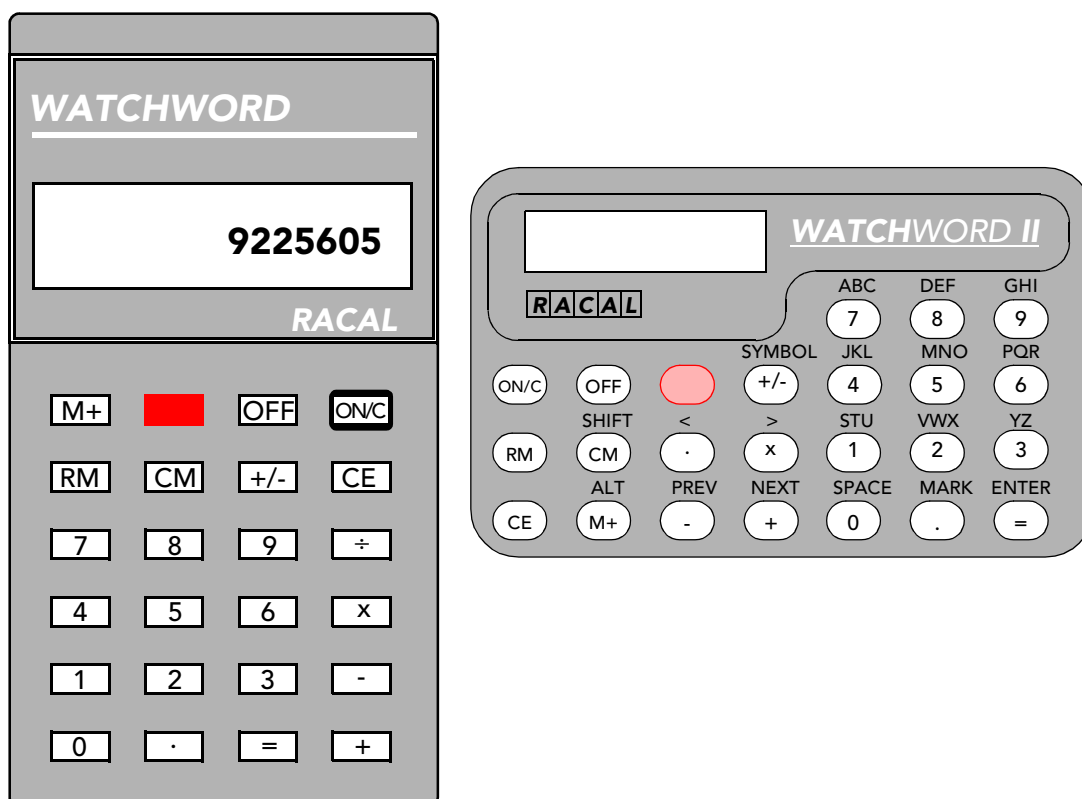
## Chapter 6 - The Watchword token

|  |     |
|--|-----|
| Watchword token description .....                                  | 6.2 |
| Using the token .....  | 6.3 |
| Installing a PIN .....   | 6.4 |
| Logging on with the Watchword token .....                          | 6.5 |
| Selecting a logon destination using PIN and KEY combinations ..... | 6.7 |

---

## Watchword token description

Your administrator has provided you with a token, similar to one of the two tokens shown below. You will need this token to gain access to your computer system as defined by your administrator.



The keys required to use the token are described below.

- ON/C** switches the Watchword token on and places it in Calculator mode (also returns to Calculator mode on completion of other functions).
- M+** places the Watchword token in Set mode and provides a series of SET prompts.
- =** stores the contents of the display and clears the display for subsequent entry.
- +** skips the currently displayed prompt to display the next prompt in sequence.
- CE** clears the contents of the display.

In addition to using the token as an authentication device, you can use the Watchword token as a standard calculator.

---

## Using the token

Your administrator will tell you when you must use the token.

The following questions and answers will guide you to the appropriate sections, which describe how you would use the token to logon to your computer - if you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure. If in doubt, contact your administrator.

**Q1** Is this the first time you have used the token?

**A1** Yes - go to *Installing a PIN* on page 6.4.  
No - go to Q2.

**Q2** Do you remember your PIN?

**A2** Yes - go to *Logging on with the Watchword token* on page 6.5.  
No - contact your administrator.

# Installing a PIN

Before you can use your token, you must enter one or two Personal Identification Numbers (PINs) into the token. A PIN is a number known only to you and should not be disclosed to anyone else.

**Note:** Your administrator will tell you whether you need one or two PINs.

Complete the steps below to enter a PIN into your token.

|               |  |  |
|---------------|--|--|
| <b>Step 1</b> | Press the <b>ON/C</b> key on your token. The token's display will look like this:  | <div><div>0.</div></div>   |
| <b>Step 2</b> | Press the <b>M+</b> key to place the token in Set mode. The display will read SET PIN 1. (If the display remains set at 0, a PIN has already been installed - contact your administrator.)   | <div><div>SET PIN 1</div></div>  |
| <b>Step 3</b> | <p>To set PIN 1, enter a number, between four and eight digits long and press the equal sign (=) to set. Remember this number as you will need it to use the token.</p> <p><b>Note:</b> If you have made a mistake in entering your PIN, DO NOT press the equals sign (=). Press the <b>CE</b> key to clear the display and start again.</p> | <div><div>SET PIN 1</div><div>12345</div><div>Example only</div></div> |
| <b>Step 4</b> | The display will now read SET PIN 2. If you do not require a second PIN, press the equal sign (=) to store nulls, otherwise complete step 3 again for PIN 2.   | <div><div>SET PIN 2</div><div>67890</div><div>Example only</div></div> |
| <b>Step 5</b> | You have successfully installed your PIN(s). Press the <b>ON/C</b> key on your token to return to calculator mode.   |  |

For security reasons, once you have set your PIN, you cannot change it. If you forget your PIN, or suspect someone else knows it, contact your administrator.

## Logging on with the Watchword token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

To access your computer system from your logon panel, carry out the following steps.

- Step 1** Enter your **USERID** and, if required, a **PASSWORD**. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

**Step 2** If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

**Step 3** A seven digit **CHALLENGE** number is displayed.

**Step 4** Press the **ON/C** key on your token. Whenever the token is turned on, it is in **Calculator** mode. The token's display will look like this:

0.

## Step 5

Press the RED key to place the token in Authentication mode. If 0 is displayed, you have not set your PINs. Go to *Installing a PIN* on page 6.4.

If two key numbers have been installed in your Watchword token, the current key number is identified in the top right of the token display by a single digit (1 or 2). Press the plus (+) key to switch between them. A selected key number can be used in conjunction with one of two PINs (if two have been set) to select one of four routes to be connected to at logon. (Refer to *Selecting a logon destination using PIN and KEY combinations* on page 6.7.)

|           |
|-----------|
| AUTH      |
| ENTER PIN |

|           |   |
|-----------|---|
| AUTH      | 1 |
| ENTER PIN |   |

## Step 6

Enter your PIN. The PIN is not shown on the token display panel, but is represented by dashes. (If you realize that you have made a mistake in entering your PIN press the **CE** key and return to step 5.)

|           |      |
|-----------|------|
| AUTH      | ---- |
| ENTER PIN |      |

## Step 7

Press the equals (=) key. The token then prompts you to enter the CHALLENGE as displayed on your terminal.

|             |
|-------------|
| AUTH        |
| ENTER CHALL |

## Step 8

Enter the CHALLENGE number into your token using the numeric keypad. As you enter the CHALLENGE number, the token displays each number entered. If you notice that you have entered the wrong number, press the CE key on your token and reenter the correct number.

|       |               |
|-------|---------------|
| AUTH  | 1 2 3 4 5 6 7 |
| ENTER | CHALL         |

Example only

## Step 9

Press the equals (=) key on your token. The token generates and displays a 7-digit RESPONSE number with a hyphen between the third and fourth digits.

|      |                 |
|------|-----------------|
| AUTH | 8 8 6 - 8 7 8 8 |
|      | RESP            |

Example only

## Step 10

Enter the RESPONSE number from your token (including hyphen) into the Response field on your terminal.

You should now gain access to your computer system. If you receive an information message, an example of which is shown below, follow the instructions in the message.

```
*****
|
| Your token expires in 5 days. Please contact your administrator if you do
| not receive your replacement token.
|
|
```

---

CKSE2425-9 Press Enter to Continue or F6 to register new token

If you are asked to register a new token, refer to *Replacing your old token with a new token* on page 10.3.

**Step 11** To return the token to Calculator mode, press the ON/C key, otherwise press the OFF key.

---

If the token displays an error symbol (E) at any time during the authentication process, press the CE key and repeat the previous step. If the error persists, consult your Administrator.

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

### Selecting a logon destination using PIN and KEY combinations

If two key numbers and two PINs have been installed in your Watchword token, a selection from four possible connect definitions may be specified an example of which is shown below.

| Key | PIN | Example application |
|-----|-----|---------------------|
| 1   | 1   | TSO                 |
| 1   | 2   | IMS                 |
| 2   | 1   | CICS                |
| 2   | 2   | NC-ACCESS           |

When you have successfully logged on, you will be connected to the appropriate application, depending on which key and PIN you used during the logon procedure.

Your administrator will advise you whether you have more than one combination set and if so, to what they refer.

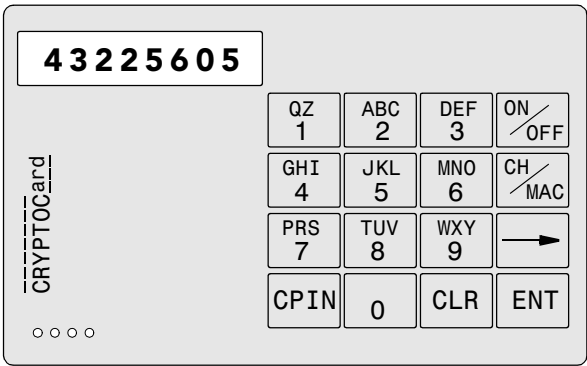
*This page intentionally left blank*

## Chapter 7 - The CRYPTOCARD token

|  |     |
|--|-----|
| CRYPTOCARD token description .....                   | 7.2 |
| Using the token .....                                | 7.3 |
| Changing the PIN provided by the administrator ..... | 7.4 |
| What to do if the token displays LOCKED .....        | 7.4 |
| Changing your PIN .....                              | 7.5 |
| Logging on with the CRYPTOCARD token .....           | 7.6 |
| Selecting a logon destination using KEYS .....       | 7.8 |

# CRYPTOCARD token description

Your administrator has provided you with a token, similar to the token shown below. You will need this token to gain access to your computer system, as defined by your administrator.



The keys required to use the token are described below.

- |               |   |
|---------------|---|
| <b>ON/OFF</b> | switches the CRYPTOCARD token on and off.   |
| <b>CPIN</b>   | allows you to change your PIN by initiating the NEW PIN installation procedure.   |
| <b>CLR</b>    | clears the contents of the display. When entry strings are longer than the display, previously entered elements are also cleared. |
| <b>ENT</b>    | signals completion of input of a string of characters and enters them into the required location.                                 |

You need a Personal Identification Number (PIN) to use the token. When your administrator gives you the token, he should also provide you with a PIN. You should change this to another PIN, known only to you. Refer to *Using the token* on page 7.3.

Your administrator can set your token with one, two or three keys. A selected key number can be used to select one of three routes to be connected to at logon. (Refer to *Selecting a logon destination using KEYS* on page 7.8.)

---

## Using the token

Your administrator will tell you when you must use the token.

The following sections describe how you would use the token to logon to your computer - if you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure.

The following questions and answers will guide you to the appropriate sections. If in doubt, contact your administrator.

**Q1** Is this the first time you have used the token?

**A1** Yes - go to Q2.  
No - go to Q3.

**Q2** Has your administrator given you the Personal Identification Number (PIN) to use with the token?

**A2** Yes - go to the section entitled *Changing the PIN provided by the administrator* on page 7.4.  
No - contact your administrator to ask for the PIN.

**Q3** Do you remember your PIN?

**A3** Yes - Go to Q4.  
No - contact your administrator.

**Q4** Do you want to change it?

**A4** Yes - go to *Changing your PIN* on page 7.5  
No - Go to *Logging on with the CRYPTOCARD token* on page 7.6.

## Changing the PIN provided by the administrator

An initial PIN is installed by the administrator. When you switch the token on for the first time you are required to enter the initial PIN in order to gain access to the token's functions.

On successful entry of the initial PIN the CRYPTOCARD token will ask you to replace the initial PIN with a new PIN that only you know. Complete the steps below to change the PIN.

---

|               |   |                     |
|---------------|---|---------------------|
| <b>Step 1</b> | Press the <b>ON/OFF</b> key. The display will request PIN entry.  | <div>PIN?</div>     |
| <b>Step 2</b> | Enter the initial PIN (as given to you by the administrator). For security reasons, asterisks (*) are displayed in place of the actual decimal digits entered.  | <div>*****</div>    |
| <b>Step 3</b> | Press the <b>ENT</b> key. The display will read NEW PIN? (If more than one key has been specified by your administrator, you will be prompted for a key number; type 1 and press the <b>ENT</b> key.) | <div>NEW PIN?</div> |
| <b>Step 4</b> | Enter the NEW PIN (displayed as asterisks (*)).   | <div>*****</div>    |
| <b>Step 5</b> | Press the <b>ENT</b> key. The display will read VERIFY.   | <div>VERIFY</div>   |
| <b>Step 6</b> | Reenter the new PIN (displayed as asterisks (*)).   | <div>*****</div>    |
| <b>Step 7</b> | Press the <b>ENT</b> key. The token will display the READY prompt.  |                     |

---

## What to do if the token displays LOCKED

If you have incorrectly entered a PIN and pressed the **ENT** key, the token may request entry again by redisplaying the PIN? prompt.

If the key is requested again, subsequent incorrect PIN entries will result in further requests for re-entry until the maximum allowable retries is reached. When this happens, your token will display LOCKED and cannot be used until reset by the administrator.

## Changing your PIN

Follow the steps listed below to change the PIN for your CRYPTOCARD token. You must know the current PIN. If you have forgotten your PIN, contact your system administrator.

---

|               |   |                 |
|---------------|---|-----------------|
| <b>Step 1</b> | Press the <b>ON/OFF</b> key. The display will request PIN entry.  | <b>PIN?</b>     |
| <b>Step 2</b> | Enter your PIN. For security reasons, asterisks (*) are displayed in place of the actual decimal digits entered.  | <b>*****</b>    |
| <b>Step 3</b> | Press the <b>ENT</b> key. The display will read READY. (If more than one key has been specified by your administrator, you will be prompted for a key number; type 1 and press the <b>ENT</b> key.) | <b>READY</b>    |
| <b>Step 4</b> | Press the <b>CPIN</b> key. The display will read NEW PIN?   | <b>New PIN?</b> |
| <b>Step 5</b> | Enter your new PIN. For security reasons, asterisks (*) are displayed in place of the actual decimal digits entered.  | <b>*****</b>    |
| <b>Step 6</b> | Press the <b>ENT</b> key. The display will read VERIFY.   | <b>VERIFY</b>   |
| <b>Step 7</b> | Reenter the new PIN (displayed as asterisks (*)).   | <b>*****</b>    |
| <b>Step 8</b> | Press the <b>ENT</b> key. The token will display the READY prompt.  |                 |

---

## Logging on with the CRYPTOCARD token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

```
Date:12/12/1997                                Host:IP01  
Time:09:00:00                                 Device:A01MS249
```

| | ||| |||||  
||| ||| |||||||  
||| ||| ||| |  
||||| ||| |||  
|||||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||  
||| ||| ||| |||

\*\*\*\*\*  
\* Personal Authentication Security System (V2.0). \*  
\* Developed by C.K.S. (IBM VTAM network software solutions). \*  
\*\*\*\*\*

USERID => TS60123 PASSWORD => TUTOR NEW PASSWORD =>  
CHALLENGE => 9225605 RESPONSE => 765-4321

The following procedure is based on the assumption that you have already replaced the initial PIN with your NEW PIN.

To access your computer system from your logon panel, carry out the following steps.

## Step 1

Enter your **USERID** and, if required, a **PASSWORD**. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

## Step 2

If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

### Step 3

A seven digit CHALLENGE number, is displayed.

## Step 4

Press the ON/OFF key on your CRYPTOCARD token. The token's display will look like this:

**PIN?**

- Step 5** Enter your PIN. For security reasons, asterisks (\*) are displayed in place of the actual digits keyed.
- Step 6** Press the **ENT** key. (If more than one key has been installed in your CRYPTOCARD token, the token display will prompt you for a key number. Enter 1, 2 or 3. Refer to *Selecting a logon destination using KEYs* on page 7.8.) The token will now show either the READY prompt (or your userid if the token was initialized with one).
- Step 7** Press the **ENT** key. The token will show an empty display.
- Step 8** Enter the CHALLENGE number from your terminal into your token.
- Step 9** Press the **ENT** key on your token. The RESPONSE code will be displayed (with or without a hyphen depending on the display format defined at initialization time).
- Enter the RESPONSE number (with the hyphen if shown) at the relevant prompt on your screen display panel and press <Enter>. You should now gain access to your computer system. If you receive an information message, an example of which is shown below, follow the instructions in the message.

\*\*\*\*\*

READY

1 2 3 4 5 6 7

ODE-2FA6

\*\*\*\*\*

Your token expires in 5 days. Please contact your administrator if you do not receive your replacement token.

CKSE2425-9 Press Enter to Continue or F6 to register new token

If you are asked to register a new token, refer to *Replacing your old token with a new token* on page 10.3.

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

## Selecting a logon destination using KEYS

If more than one key has been installed in your CRYPTOCARD token, a selection from three possible connect definitions may be specified, an example of which is shown below.

| Key | Example application |
|-----|---------------------|
| 1   | TSO                 |
| 2   | CICS                |
| 3   | NC-ACCESS           |

When you have successfully logged on, you will be connected to the appropriate application, depending on which key you used during the logon procedure.

Your administrator will advise you whether you have more than one key set and if so, to what they refer.

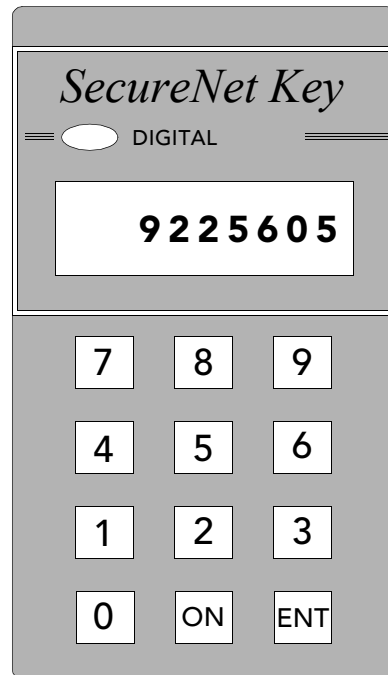
## Chapter 8 - The SecureNet Key token

|   |     |
|---|-----|
| SecureNet Key token description .....     | 8.2 |
| Using the token .....                     | 8.3 |
| Loading the PIN .....                     | 8.4 |
| Logging on with the SecureNet token ..... | 8.5 |

---

## SecureNet Key token description

Your administrator has provided you with a token, similar to the token shown below. You will need this token to gain access to your computer system as defined by your administrator



The following two simple keypad functions are used.

**ON** switches the SecureNet token on and displays a two character readiness code. The ON key also performs a reset function.

**ENT** causes the token to read data entered in the display.

You need a Personal Identification Number (PIN) to use the token. When your administrator gives you the token, he will either provide you with a PIN, or tell you to load one yourself. Refer to *Using the token* on page 8.3.

---

## Using the token

Your administrator will tell you when you must use the token.

The following sections describe how you would use the token to logon to your computer - if you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure.

The following questions and answers will guide you to the appropriate sections. If in doubt, contact your administrator.

**Q1** Is this the first time you have used the token?

**A1** Yes - go to Q2.  
No - go to Q3.

**Q2** Has your administrator given you a Personal Identification Number (PIN) to use with the token?

**A2** Yes - go to the section entitled *Logging on with the SecureNet token* on page 8.5.  
No - go to the section entitled *Loading the PIN* on page 8.4.

**Q3** Do you remember your PIN?

**A3** Yes - Go to the section entitled *Logging on with the SecureNet token* on page 8.5.  
No - contact your administrator.

## Loading the PIN

Complete the following steps to load a PIN into your token.

---

|               |  |                            |
|---------------|--|----------------------------|
| <b>Step 1</b> | Press the ON key. The display will read E2.<br><br>(If the display reads<br>EP a PIN has already been installed; if you<br>do not know the PIN, contact your<br>administrator.<br>E0 contact your administrator)   | <div>E2      - - - -</div> |
| <b>Step 2</b> | Enter a PIN between 4 and 16 digits long.<br>Remember this number as you will need it to<br>use the token. (The number is not displayed<br>but is represented by lower case letters.)  | <div>o o o o</div>         |
| <b>Step 3</b> | Press <b>ENT</b> . The display will read E3. (If the<br>display still reads E2, you have not typed in<br>the correct number of digits; repeat step 2<br>again.)  | <div>E3      - - - -</div> |
| <b>Step 4</b> | Type in exactly the same PIN again for<br>verification and press <b>ENT</b> . The display<br>should read EP. You have successfully<br>loaded the PIN and can now use the token<br>to gain access to your computer system.<br>Refer to <i>Logging on with the SecureNet<br/>token</i> on page 8.5<br>(If the display reverts to E3, you have<br>mistyped the PIN and verification has failed.<br>Repeat the process from Step 2.) | <div>EP      - - - -</div> |

---

## Logging on with the SecureNet token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

To access your computer system from your logon panel, carry out the following steps.

### Step 1

Enter your **USERID** and, if required, a **PASSWORD**. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

## Step 2

If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

### Step 3

A CHALLENGE number is displayed at the relevant prompt on your screen.

## Step 4

Press the ON key on your token. The token's display will look like this:

EP . . . .

- Step 5** Enter your PIN. The PIN is not displayed, but is represented by a lower case letters. If you realize you have made a mistake in entering your PIN, press the **ON** key and start again.
- Step 6** Press the **ENT** key. The display will show a readiness code of Ed. If the wrong PIN has been entered the display will show Error.
- Step 7** Enter the **CHALLENGE** number from your terminal into the token.
- Step 8** Press the **ENT** key. The token generates and displays a RESPONSE number.
- Enter the response number at the relevant prompt on your logon panel. You should now gain access to your computer system. If you receive an information message, an example of which is shown below, follow the instructions in the message.

```
*****
|
| Your token expires in 5 days. Please contact your administrator if you do
| not receive your replacement token.
|
|*****
```

---

CKSE2425-9 Press Enter to Continue or F6 to register new token

If you are asked to register a new token,  
refer to *Replacing your old token with a new  
token* on page 10.3.

---

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

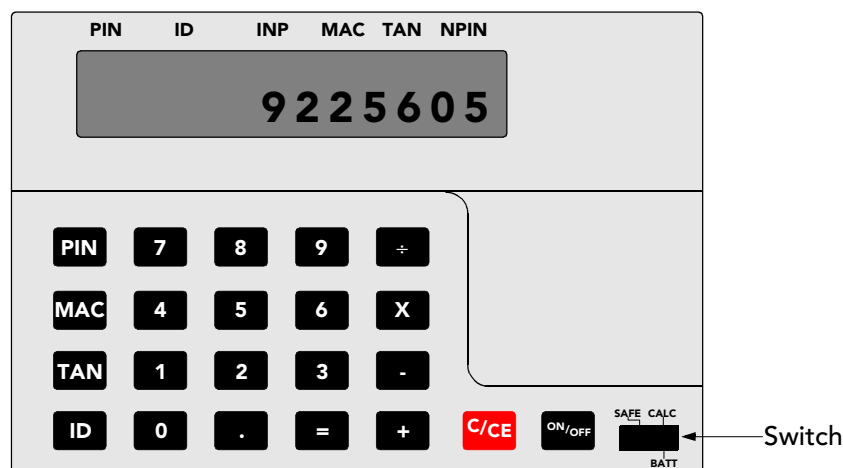
## Chapter 9 - The Safe S220 token

|   |     |
|---|-----|
| Safe S220 token description .....         | 9.2 |
| Using the token .....                     | 9.3 |
| Changing the PIN .....                    | 9.4 |
| Logging on with the Safe S220 token ..... | 9.5 |

---

## Safe S220 token description

Your administrator has provided you with a token, similar to the token shown below. You will need this token to gain access to your computer system, as defined by your administrator.



The keys required to use the token are described below.

|               |   |
|---------------|---|
| <b>ON/OFF</b> | switches the S220 token on and off.                       |
| <b>PIN</b>    | stores the contents of the display into the PIN location. |
| <b>MAC</b>    | memory access key.  |
| <b>C/CE</b>   | clears the contents of the display.                       |
| <b>Switch</b> | Switches the token into SAFE or CALCulator mode.          |

You need a Personal Identification Number (PIN) to use the token. When your administrator gives you the token, he should also provide you with a PIN. You should change this to another PIN, known only to you. Refer to *Using the token* on page 9.3.

---

## Using the token

Your administrator will tell you when you must use the token.

The following sections describe how you would use the token to logon to your computer - if you are using the token to authorize you to carry out a particular function, omit the steps which describe the logon procedure.

The following questions and answers will guide you to the appropriate sections. If in doubt, contact your administrator.

**Q1** Is this the first time you have used the token?

**A1** Yes - go to Q2.  
No - go to Q3.

**Q2** Has your administrator given you the Personal Identification Number (PIN) to use with the token?

**A2** Yes - go to the section entitled *Changing the PIN* on page 9.4.  
No - contact your administrator to ask for the PIN.

**Q3** Do you remember the PIN?

**A3** Yes - Go to *Logging on with the Safe S220 token* on page 9.5  
No - contact your administrator.

## Changing the PIN

When you change the PIN, you must enter the new PIN at the **NEW PIN** prompt on the logon panel at the time it is changed. The change must therefore be made during a logon.

Complete the following steps to change the S220 PIN:

---

|                |  |   |     |             |      |     |     |      |   |  |  |  |             |  |
|----------------|--|---|-----|-------------|------|-----|-----|------|---|--|--|--|-------------|--|
| <b>Step 1</b>  | Ensure the token is switched to SAFE mode.   |   |     |             |      |     |     |      |   |  |  |  |             |  |
| <b>Step 2</b>  | Press the ON/OFF key on the token. A question mark (?) will be displayed under PIN.                    | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>?</td><td></td><td></td><td></td><td></td><td></td></tr></table>            | PIN | ID          | INP  | MAC | TAN | NPIN | ? |  |  |  |             |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| ?              |  |   |     |             |      |     |     |      |   |  |  |  |             |  |
| <b>Step 3</b>  | Enter the current PIN number.  | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>?</td><td></td><td></td><td></td><td>- - - -</td><td></td></tr></table>     | PIN | ID          | INP  | MAC | TAN | NPIN | ? |  |  |  | - - - -     |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| ?              |  |   |     | - - - -     |      |     |     |      |   |  |  |  |             |  |
| <b>Step 4</b>  | Press the PIN key. The display will blank out. Wait for a few seconds until the display is refreshed.  | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>=</td><td></td><td></td><td></td><td>1 2 3 4 5 6</td><td></td></tr></table> | PIN | ID          | INP  | MAC | TAN | NPIN | = |  |  |  | 1 2 3 4 5 6 |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| =              |  |   |     | 1 2 3 4 5 6 |      |     |     |      |   |  |  |  |             |  |
| <b>Step 5</b>  | Press the PIN key a second time.   | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>?</td><td></td><td></td><td></td><td></td><td></td></tr></table>            | PIN | ID          | INP  | MAC | TAN | NPIN | ? |  |  |  |             |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| ?              |  |   |     |             |      |     |     |      |   |  |  |  |             |  |
| <b>Step 6</b>  | Press the TAN key.   | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td></td><td></td><td></td><td></td><td>?</td><td></td></tr></table>            | PIN | ID          | INP  | MAC | TAN | NPIN |   |  |  |  | ?           |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
|                |  |   |     | ?           |      |     |     |      |   |  |  |  |             |  |
| <b>Step 7</b>  | Enter the new PIN number.  | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>?</td><td></td><td></td><td></td><td>1 2 3 4 5</td><td></td></tr></table>   | PIN | ID          | INP  | MAC | TAN | NPIN | ? |  |  |  | 1 2 3 4 5   |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| ?              |  |   |     | 1 2 3 4 5   |      |     |     |      |   |  |  |  |             |  |
| <b>Step 8</b>  | Press the PIN key. The display will blank out. Wait for a few seconds until the display is refreshed.  | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>=</td><td></td><td></td><td></td><td>9 8 5 8 9 8</td><td></td></tr></table> | PIN | ID          | INP  | MAC | TAN | NPIN | = |  |  |  | 9 8 5 8 9 8 |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| =              |  |   |     | 9 8 5 8 9 8 |      |     |     |      |   |  |  |  |             |  |
| <b>Step 9</b>  | Press the MAC key.   | <table><tr><td>PIN</td><td>ID</td><td>INP</td><td>MAC</td><td>TAN</td><td>NPIN</td></tr><tr><td>=</td><td></td><td></td><td></td><td>1 2 3 4 5</td><td></td></tr></table>   | PIN | ID          | INP  | MAC | TAN | NPIN | = |  |  |  | 1 2 3 4 5   |  |
| PIN            | ID   | INP   | MAC | TAN         | NPIN |     |     |      |   |  |  |  |             |  |
| =              |  |   |     | 1 2 3 4 5   |      |     |     |      |   |  |  |  |             |  |
| <b>Step 10</b> | The new PIN number is now installed. Enter the number at the <b>NEW PIN</b> prompt on the logon panel. |   |     |             |      |     |     |      |   |  |  |  |             |  |

---

## Logging on with the Safe S220 token

Carry out the normal steps to display the logon panel on your computer. An example panel is shown below. The exact layout will depend on how your system has been set up.

[illegible]

To access your computer system from your logon panel, carry out the steps below.

### Step 1

Enter your **USERID** and, if required, a **PASSWORD**. (If this is the first time you have tried to logon using your token, you may be presented with a series of instruction panels, advising how to use the token.)

## Step 2

If this is the first time you have used the token, you may be presented with a panel asking you to register your use of the token. If so, go to *Registering your token* on page 10.2, carry out the steps there, before returning to complete step 3.

If this is not the first time you have used the token, or you have not been asked for registration details, carry on with Step 3.

### Step 3

Ensure that your token is switched to SAFE mode.

### Step 4

Press the **ON/OFF** key on your token. The token's display will look like this:

| PIN | ID | INP | MAC | TAN | NPIN |
|-----|----|-----|-----|-----|------|
| ?   |    |     |     |     |      |

Enter your PIN number.

| PIN | ID | INP | MAC | TAN | NPIN |
|-----|----|-----|-----|-----|------|
| ?   |    |     | -   | -   | -    |

Press the **PIN** key. This will generate your SPIN. (If the token display shows an E under PIN, you have entered the wrong PIN.)

| PIN | ID | INP | MAC | TAN | NPIN |
|-----|----|-----|-----|-----|------|
| =   |    |     |     |     |      |
|     |    | 1   | 1   | 2   | 2    |
|     |    |     |     | 2   | 1    |

**Example only**

Enter the SPIN number generated by your S220 token at the SPIN prompt and press <Enter>. You should now gain access to the system.

If you receive an information message, an example of which is shown below, follow the instructions in the message.

\*\*\*\*\*

Your token expires in 5 days. Please contact your administrator if you do not receive your replacement token.

CKSE2425-9 Press Enter to Continue or F6 to register new token

If you are asked to register a new token, refer to *Replacing your old token with a new token* on page 10.3.

If the token displays an error symbol (E) at any time during the authentication process, press the C/CE key and repeat the procedure. If the error persists, consult your Administrator.

If you receive an ACCESS DENIED message, you may have entered incorrect data. Try to logon again. If you do not know why you have been denied access, contact your administrator for advice.

## Chapter 10 - Token registration and replacement

|   |      |
|---|------|
| Registering your token .....                    | 10.2 |
| Replacing your old token with a new token ..... | 10.3 |

---

## Registering your token

When you first use your token, you may be required to register it yourself; if so, the TOKEN SELF REGISTRATION panel is displayed at logon, an example of which is shown below.

**Note:** The text in this panel may change, depending on your registration requirements.

```
Date:12/12/1997          TOKEN SELF REGISTRATION          Userid:TSG0001
Time:09:00                Terminal:A01MS249

Your userid requires you to log on using a token. If you have not been provided
with a token, consult your administrator.
Before you are able to log on using your token, certain information is required
to identify you with the device you are using.
Listed below are the types of device which are currently supported. Enter S
alongside the token type which you wish to use. Enter the token number of the
device at the 'Token number =>' prompt.

S TOKEN TYPE
ActivCard token (ActivCard)
DES Challenge-response token - RB (CRYPTOCARD)
Safe S220 token (Racal)
Digipass token (Digipass)
SecurID standard token (Security Dynamics)
SecurID Pinpad token (Security Dynamics)
SecureNet Key token (Digital Pathways)
Watchword token (Racal)
Token number => _____

CKSE1064-6 Self-registration in progress
F3=End
```

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Identify the token type you want to use by entering S in the S column, against the type of token that the administrator has given you.   |
| <b>Step 2</b> | Press the tab key until the cursor is in the <b>Token number</b> field and enter the token serial number which you will find on the back of the token.                                   |
| <b>Step 3</b> | If you successfully register your token, the system will prompt you for details from the token. Return to the chapter describing your token and follow the instructions on how to logon. |
-

---

## Replacing your old token with a new token

If your administrator provides you with a new token, to replace your current token, you will be prompted by the system to provide the necessary details. This will take the form of a message issued at logon, prompting you to press <F6> to register a new token. When you press <F6>, the TOKEN SELF REGISTRATION panel is displayed, an example of which is shown below.

**Note:** The text in this panel may change, depending on your registration requirements.

Date:12/12/1997Time:17:00

TOKEN SELF REGISTRATION

Userid:TSG0001Terminal:A01MS266

Your userid requires you to use a token during logon and your current token will soon expire. Your Administrator should have issued you with a replacement token. Listed below are the types of token device currently supported. Enter S alongside the type of your replacement token and the token serial number, without any preceding letters if any, at the prompt below. Press <F3> to register the replacement token which will be required at your next logon. Return your old token to your Administrator.

S TOKEN TYPE  
SecurID Pinpad token (Security Dynamics)

Token number => \_\_\_\_\_

F3=End F12=Can

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Identify the new token type you want to use by entering S in the S column, against the type of token that the administrator has given you.  |
| <b>Step 2</b> | Press the tab key until the cursor is in the <b>Token number</b> field and enter the new token serial number which you will find on the back of the token.                                      |
| <b>Step 3</b> | If you successfully register your token, the system will prompt you for details from the new token. Return the old token to your administrator and use the new token for all subsequent logons. |
-

*This page intentionally left blank*

# Index

## A

ActivCard token  
    changing the PIN 4.3  
    description 4.2  
    entering a Challenge 4.5  
    entering a Response 4.5  
    how to use 4.3  
    LOCKED display 4.6  
    setting up initial PIN 4.3  
assigning yourself to a token 1.2

## C

CRYPTOCARD token  
    changing the PIN 7.4, 7.5  
    description 7.2  
    LOCKED display 7.4  
    logging on with 7.6  
    using 7.3

## D

death date of SecurID P tokens 3.6  
Digipass token  
    changing the initial PIN (IPIN) 5.4  
    description 5.2  
    entering a response 5.6  
    how to use 5.3

## E

expiry of SecurID P tokens 3.6  
expiry of tokens 1.3

## H

home computer, specifying 1.3

## I

initial PIN  
    Digipass token 5.2

## K

Key  
    using to select logon destination 6.7, 7.8

## L

LOCKED display  
    ActivCard token 4.6  
    CRYPTOCARD token 7.4

logging on with  
    the ActivCard token 4.4  
    the CRYPTOCARD token 7.6  
    the Digipass token 5.5  
    the Safe S220 token 9.5  
    the SecureNet token 8.5  
    the SecurID A token 2.3  
    the SecurID P card 3.5  
    the Watchword token 6.5  
logon destination selection with  
    the CRYPTOCARD token 7.8  
    the Watchword token 6.7

## P

passcodes, introduction to 1.3  
Personal Identification Number see *PIN*  
*PIN*  
    ActivCard token  
        changing for 4.3  
        setting up initial 4.3  
    CRYPTOCARD token  
        changing for 7.5  
        changing initial 7.4  
    Digipass token  
        changing initial 5.4  
    introduction to 1.2  
    Safe S220 token  
        changing for 9.4  
    SecureNet Key token  
        loading for 8.4  
    SecurID P token  
        changing for 3.5  
        setting up initial 3.4  
    Watchword token  
        installing 6.4  
        using to select logon destination 6.7  
*PRN*  
    SecurID A token 2.2  
    SecurID P token 3.2, 3.4  
Pseudo Random Number see *PRN*

## R

registering your token 10.2  
replacing your old token with a new token 10.3

## S

Safe S220 token  
    changing the PIN 9.4  
    description 9.2  
    logging on with 9.5  
    using 9.3  
SecureNet Key token  
    description 8.2  
    loading the PIN 8.4  
    logging on with 8.5  
    using 8.3  
SecurID A token  
    description 2.2  
    logging on with 2.3

- SecurID P token
  - changing the PIN 3.5
  - description 3.2
  - expiry 3.6
  - logging on with 3.5
  - setting up the initial PIN 3.4
  - using 3.3
- selecting a logon destination
  - using KEYs 7.8
  - using PIN and KEY combinations 6.7

## T

- token self registration 10.2
- tokens
  - ActivCard 4.2
  - assigning yourself to 1.2
  - CRYPTOCARD 7.2
  - Digipass 5.2
  - expiry 1.3
  - introduction to 1.2
  - registering 10.2
  - replacing old with new 10.3
  - Safe S220 9.2
  - SecureNet Key 8.2
  - SecurID A 2.2
  - SecurID P 3.2
  - using at logon 1.2
  - using, other than at logon 1.2
  - Watchword 6.2

## U

- using a token at logon 1.2
- using a token other than at logon 1.2
- using KEYs to select a logon destination 7.8
- using passcodes 1.3
- using PIN and KEY combinations to select logon destination 6.7

## W

- Watchword token
  - installing a PIN 6.4
  - logging on with 6.5
  - selecting a logon destination 6.7
  - using 6.3

# Reader's Comment Form

If you find any discrepancy in the information contained in this publication, please complete this form and mail it to the address below.

The authors may use, or distribute, any of the information you supply in any way they consider appropriate without incurring any obligation whatsoever.

Publication number PAU0001.003 - Third Edition (October 2001)

Please write your comments below and on the following page and return this form to the

Documentation Manager  
PassGo Technologies Ltd.  
Horton Manor  
Ilminster, Somerset  
TA19 9PY  
England

***Reader's Comment Form***

N  
C  
  
P  
A  
S  
S  
  
A  
u  
t  
h  
e  
n  
t  
i  
c  
a  
t  
o  
r  
  
U  
s  
e  
r  
  
G  
u  
i  
d  
e